IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WSOU INVESTMENTS, LLC D/B/A BRAZOS LICENSING AND DEVELOPMENT, Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	Case No. 6:21-CV-00128-ADA JURY TRIAL DEMANDED

DEFENDANT CISCO SYSTEMS, INC.'S OPENING CLAIM CONSTRUCTION BRIEF REGARDING U.S. PATENT NOS. 7,443,859; 8,191,106; 8,989,216; AND 9,357,014

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF ABBREVIATIONS

Abbreviation	Meaning
’014 patent	U.S. Patent No. 9,357,014
’106 patent	U.S. Patent No. 8,191,106
’216 patent	U.S. Patent No. 8,989,216
’859 patent	U.S. Patent No. 7,443,859
3GPP	3rd Generation Partnership Project
APN	Access Point Name
AVP	Attribute Value Pair
Cisco	Defendant Cisco Systems, Inc.
CSL	Connected Services Layer
CSS	Connected Services Stack
Dkt.	Docket Number
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Services
ICME	Inter-technology Change-off Monitoring Entity
NAT	Network Address Translator
POSA	Person of Ordinary Skill in the Art
SGSN	Serving GPRS Support Node
WSOU	Plaintiff WSOU Investments, LLC D/B/A Brazos Licensing and Development

TABLE OF EXHIBITS[1]

Exhibit	Document
Ex. 1	WSOU's Preliminary Infringement Contentions (June 23, 2021)
Ex. 2	3GPP TS 23.060 v. 4.2.0, General Packet Radio Service (GPRS); Service description; Stage 2 (Release 4) (2001) (CISCO-WSOU-CC-00000001)
Ex. 3	3GPP TS 24.008 v. 4.4.0, General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (Release 4) (2001) (CISCO-WSOU-CC-00000002)
Ex. 4	3GPP TS 29.060 v. 4.2.0, Mobile radio interface layer 3 specification; Core Network Protocols - Stage 3 (Release 4) (2001) (CISCO-WSOU-CC-00000004)
Ex. 5	'859 Patent Prosecution History
Ex. 6	RFC 1918 "Address Allocations for Private Internets" (Feb. 1996) (CISCO-WSOU-CC-00000006)
Ex. 7	RFC 3022 "Traditional IP Network Address Translator (Traditional NAT)" (Jan. 2001) (CISCO-WSOU-CC-00000003)
Ex. 8	WSOU's Identification of Claim Terms for Construction (Sept. 1, 2021)
Ex. 9	Cisco Networking Academy "Lab – Researching Converged Network Services (Instructor Version)" (WSOU-CISCO001853)
Ex. 10	RFC 3588 "Diameter Base Protocol" (Sept. 2003) (CISCO-WSOU-CC-00000011)
Ex. 11	'216 Patent Prosecution History
Ex. 12	U.S. Patent No. 7,304,563
Ex. 13	U.S. Patent No. 7,872,973
Ex. 14	E-mail Correspondence from WSOU to Cisco (Sept. 29, 2021)
Ex. 15	Mohammed M. Alani, "Guide to OSI and TCP/IP Models" (2014) (CISCO-WSOU-CC-00000010).
Ex. 16	AWS Lambda (WSOU-CISCO003161-3169)

[1] Exhibits are attached to the Declaration of Brian A. Rosenthal in Support of Cisco's Opening Claim Construction Brief.

I. Introduction

Cisco proposes constructions for eight of the ten technical terms in dispute across the four asserted patents that are rooted squarely in the plain language of the claims, as informed by the specification. Cisco has taken care to avoid importing limitations from preferred embodiments, and instead proposes constructions that capture precisely what a person skilled in the art would understand they mean based on reading the claims—no more and no less. For the remaining two terms (in the '216 patent), Cisco does not propose a construction because those terms are hopelessly indefinite.

WSOU, on the other hand, seeks to avoid construing any terms at all from the four patents. It does not even propose a construction for the single term it said should be construed during the parties' exchanges. Instead, WSOU seeks to keep the four patents as malleable as possible so that it can maintain its non-credible infringement theories in this case. Indeed, during meet and confer discussions, when Cisco repeatedly asked what aspects of WSOU's constructions were objectionable, WSOU had no answer, instead simply repeating that it does not think any construction is necessary.

Cisco requests that the Court construe the terms to mean what they say, as reflected in its proposed constructions.

II. U.S. Patent No. 7,443,859

The '859 patent relates generally to assigning public or private IP addresses in a General Packet Radio Services (GPRS) cellular network. Figure 5 (annotated below) depicts a GPRS network:

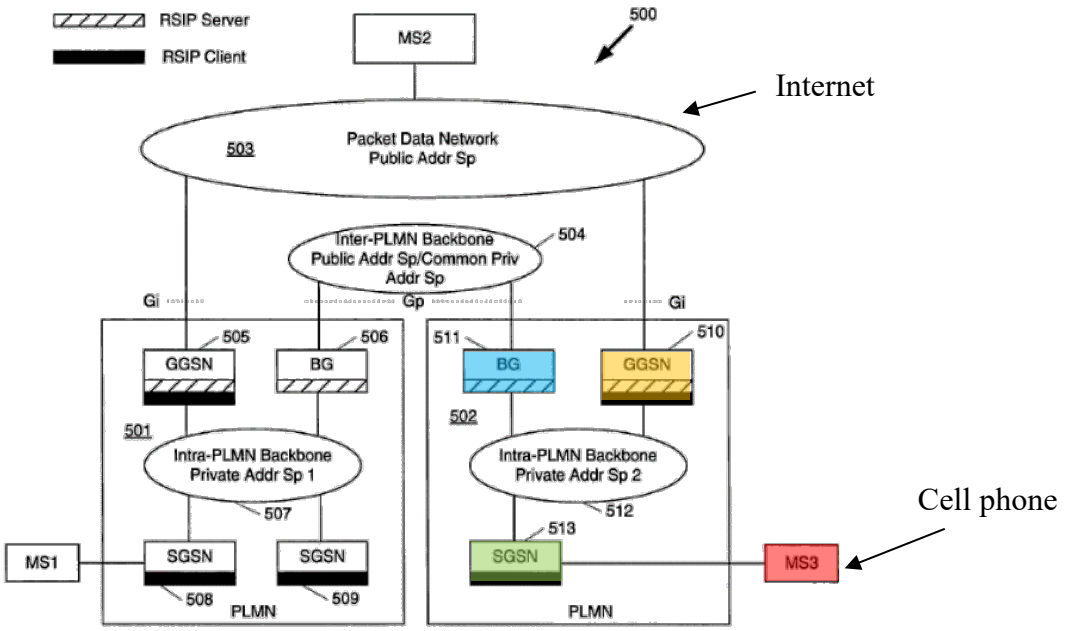

FIG. 5

As shown above, a cell phone (MS) connects to the Internet via a network node called a Serving GPRS Support Node (SGSN), which connects to either a Gateway GPRS Support Node (GGSN) or Border Gateway (BG).

As the patent explains, the different messages sent among these network components were defined in the GPRS standard that existed at the time of the patent filing. '859 patent, 3:28-46, Figs. 4a-4d. The patent also explains that each cell phone is assigned an IP address to connect to the Internet. However, as the patent explains, there are a limited number of IP addresses available. *Id.*, 1:16-17. To conserve IP addresses, GPRS networks can use "private" IP addresses that are unique only within the network that assigns them—*i.e.*, private IP addresses may be re-used in other networks on the Internet. *Id.*, 1:14-29. Those private IP addresses are assigned within a preset range of IP addresses defined in Internet standards. *Id.*, 1:16-32.

Because private IP addresses are not unique across the Internet, the private address must be translated to communicate with devices outside of the network. *Id.*, 1:29-44. Traditionally, the address translation is done by a Network Address Translator or "NAT" (which is the GGSN in a

GPRS network). *Id*., 2:44-2:5, Fig. 1. Although private IP addresses help conserve IP addresses, the patent states that they do not allow for end-to-end security because the NAT needs to translate IP addresses between private and public addresses. *Id*., 2:36-3:3, 3:51-55.

According to the patent, it was known that public addresses (*i.e.*, those that are unique across the Internet) could be used for certain cell phones for which end-to-end security is required, but the GPRS standard does not specify whether private or public IP addresses are assigned to devices. *Id*., 3:37-55, 3:4-10. To solve this alleged deficiency in the existing GPRS standard, the patent purports to use an existing field in the existing GPRS messages to explicitly state whether the cell phone should be assigned a public or a private IP address. *Id*., 3:47-62. Specifically, one or more bits of the existing "Access Point Name (APN) field" in the message sent from the cell phone to the SGSN and the message from the SGSN to the GGSN or BG is used to explicitly request a public or private IP address. *Id*., 7:1-22. This way, if the cell phone requires end-to-end security for its communications, it could explicitly request a public IP address to enable that security. *Id.*

A. "APN (Access Point Name) field" / "APN field" (Claims 1-5, 7, 9-11, 15-17, 22-24, 26)

Cisco's Proposal	WSOU's Proposal
Specific field identified as "Access Point Name" that contains the name of the access point	Plain and ordinary meaning

Cisco's proposed construction defines the "APN field" to be what it is: a specific field—called the "Access Point Name" (APN) field—in specific messages defined by the GPRS standard. That "Access Point Name" field, unsurprisingly, contains the name of the access point. The totality of the intrinsic and extrinsic evidence supports this construction. The construction is necessary because WSOU seeks to read this limitation on an entirely different field that happens to have the

letters "APN" in the title.[2] The Court should construe this term in the same way that it would be interpreted by a person skilled in the art to mean the specific APN field defined in the standards.

The claims themselves explicitly recite the APN field by name, as being part of specifically named and existing GPRS messages. For example, claim 1 recites the "***APN (Access Point Name) field***" in the "Activate PDP Context Request" that is sent from the MS to the SGSN in a GPRS network.[3] Similarly, claim 2 recites the "***APN field***" in the "Create PDP Context Request" message that is sent from the SGSN to the GGSN. Thus, the claims refer to a specifically named field in a specifically named message.

The background section of the patent makes clear that the claimed APN field is an already-known field in these GPRS standard messages. *See id.*, 3:28-46. These preexisting GPRS messages are depicted in Figure 4:

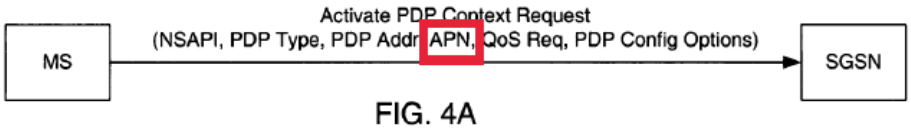

FIG. 4A

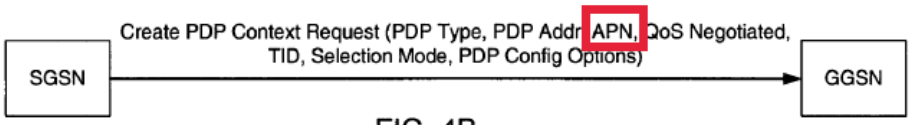

FIG. 4B

As shown above, the message from the cell phone (MS) to the SGSN is called "Activate PDP

[2] In its infringement contentions, WSOU alleges that another field—**not** the APN field in the standard—is the claimed APN field. *See* Ex. 1 (WSOU's Preliminary Infringement Contentions), Ex. B, 2-3 (alleging infringement by the separate "APN Restriction" field that is not even a part of the Activate PDP Context Request). *See Wilson Sporting Goods Co. v. Hillerich & Bradsby Co.*, 442 F.3d 1322, 1327 (Fed. Cir. 2006) ("Although the construction of the claim is independent of the device charged with infringement, it is convenient for the court to concentrate on those aspects of the claim whose relation to the accused device is in dispute." (quotation omitted)).

[3] All emphasis added unless indicated otherwise.

Context Request" and includes a field called "APN." Similarly, the message from the SGSN to the GGSN or BG is called "Create PDP Context Request" and also includes a field called "APN." These are the same fields that are recited in the claims, as set forth above.

Indeed, according to the patent, "the ***present invention*** provides an MS that utilizes the ***APN field of the Activate PDP Context Request message*** as an extensible field by inserting information into the APN field for requesting either a public or a private address assignment." *Id.*, 7:7-11. In other words, the patent itself states that the ***present invention*** utilizes the preexisting APN field of the standard and adds information into it; it does not create a new field or use one of the other fields in the messages depicted in Figure 4. This description of the "present invention" confirms the plain and ordinary meaning of the APN field as a specific field in standard messages. *See, e.g.*, *Marine Polymer Techs., Inc. v. HemCon, Inc.*, 672 F.3d 1350, 1359 (Fed. Cir. 2012) (holding use of "the present invention" limits the claims); *Modine Mfg. Co., v. Int'l Trade Comm'n*, 75 F.3d 1545, 1551 (Fed. Cir. 1996) ("[W]hen the preferred embodiment is described in the specification as the invention itself, the claims are not necessarily entitled to a scope broader than that embodiment.").

The GPRS standards existing at the time of the alleged invention to which the '859 patent refers also confirm that the APN field is a specific field referred to as the APN field. *See* Ex. 2 (3GPP TS 23.060 v. 4.2.0), 160-61; Ex. 3 (3GPP TS 24.008 v. 4.4.0), 384; Ex. 4 (3GPP TS 29.060 v. 4.2.0), 62. For example, 3GPP TS 24.008 v. 4.4.0, which was published in 2001 before the priority date of the '859 patent, explains that the APN field contains information that identifies the name of a specific access point.

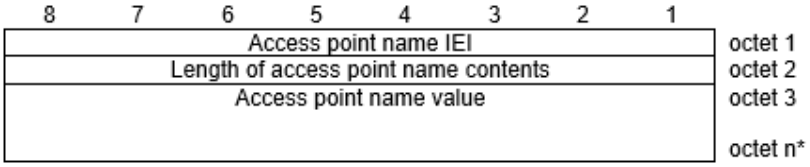

Figure 10.5.134/3GPP TS 24.008: Access *point name* information element

Ex. 3 (3GPP TS 24.008 v. 4.4.0), 384; *see* Ex. 4 (3GPP TS 29.060 v. 4.2.0), 64 ("The Access Point Name contains a logical name that is the APN Network Identifier (see 3GPP TS 23.060)."). The standard also explains that the APN field is used by the SGSN to select the GGSN and the '859 patent confirms this same use of the APN field. *Compare* '859 patent, 7:23-25, *with* Ex. 2 (3GPP TS 23.060 v. 4.2.0), 174 ("APN and GGSN Selection").

In sum, the totality of the intrinsic and extrinsic evidence confirms that the plain and ordinary meaning of the "APN field" refers to a specific, well-known field with specific information in certain messages of the GPRS standard. Cisco respectfully requests the Court adopt its proposed construction.

B. "explicitly indicates requesting either a private network address or a public network address" (Claims 1, 8-11, 15, 21-24, 26)

Cisco's Proposal	WSOU's Proposal
Plain and ordinary meaning (particular bit or bits indicate requesting either a private or public network address, rather than determining the desired public or private assignment based upon the indicated access point)	Plain and ordinary meaning

Cisco's proposed construction is consistent with the plain and ordinary meaning of "explicit" and is confirmed by the totality of the intrinsic record, including the specification and the prosecution history. In one example, the applicant specifically disavowed any implicit requests by adding during prosecution the requirement that the request be "explicit" to avoid the prior art. WSOU cannot be allowed to reclaim implied requests under the guise of a plain and ordinary meaning construction.

Each independent claim requires that the APN field contains information that "***explicitly*** indicates requesting either a private network address or a public network address to be assigned to a [MS]." '859 patent, cls. 1, 9, 10, 11, 15, 22, 23, 24, 26. Consistent with the plain and ordinary meaning of ***explicit***, the specification explains that "an ***explicit*** indication" can be "a particular bit (or bits) of the APN field being set." *Id*., 7:13-14. In other words, for there to be an ***explicit*** request something within the APN field itself must explicitly specify whether the IP address will be public or private. This is consistent with Cisco's proposed explanation of the plain and ordinary meaning.

The patent also distinguishes an explicit request from an implicit indication, where the request for a private or public network address can be implied or inferred from other information, such as "the address of a GGSN contained in the APN field." *Id*., 7:14-15. This distinction between "explicit" and "implicit" requests in the specification is consistent with the ordinary usage of these terms. For example, an "explicit" request to take out the garbage would be an explicit statement like: "Please take out the trash." An "implicit" request, on the other hand, could be a more general statement like "Today is Sunday." One would have to know that Sunday is trash day to then infer that the trash must be taken out.

The plain meaning of "explicitly" is further confirmed in the prosecution history. During prosecution, the applicant amended the claims to recite "an APN field containing information that explicitly indicates requesting ~~relating to a request for~~ one of a private network address and a public network address to be assigned to the mobile station." Ex. 5 ('859 Patent Prosecution History), 203 (January 23, 2007 Amendment), 241 (March 5, 2007 Amendment), 274 (August 23, 2007 Amendment). According to the applicant, the prior art did not "teach[] or suggest[] assignment of a private or a public network address be based on information in the APN field that

explicitly indicates requesting one of a private network address and a public network address as requested by the mobile station." *Id*., 229 (March 5, 2007 Applicant Remarks) (emphasis in original). The applicant admitted that one of the prior art references disclosed "an APN field containing information identifying a destination network gateway," but argued that merely specifying a destination gateway does not explicitly indicate whether the IP address should be private or public. *Id*., 230. As set forth above, this is fully consistent with the ordinary meaning of the word "explicitly" and therefore supports Cisco's construction. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005).

While Cisco need not establish prosecution disclaimer, since the prosecution history is consistent with the plain language, here the prosecution also rises to the level of a disclaimer. To get around the prior art taught and implied request, the applicant added the requirement that the request be "explicit," and distinguished it from an implicit request. WSOU cannot be allowed to reclaim implied requests under the guise of a plain and ordinary meaning construction. *See Tech. Props. Ltd. LLC v. Huawei Techs. Co.*, 849 F.3d 1349, 1358 (Fed. Cir. 2017) (affirming disclaimer where applicant argued during prosecution that prior art was "'specifically distinguished from the instant case'" (citation omitted)).

Cisco's proposed construction includes a parenthetical that explains what it means for a request to be explicit, and distinguishes from an implicit request, as the applicant did during prosecution. Cisco respectfully requests the Court adopt its proposed construction.

C. "a private network address" (Claims 1-5, 7-11, 15-17, 21-24, 26)

Cisco's Proposal	WSOU's Proposal
An address that is only visible within the network that assigned it	Plain and ordinary meaning

Cisco's proposed construction is consistent with the ordinary meaning of "private network

address" and the stated purpose of the "present invention" in the patent. The claims recite "a ***private*** network address or a ***public*** network address." Consistent with the plain and ordinary meanings of "public" and "private," a public address refers to an address publicly visible outside a network (*i.e.*, an address that is publicly accessible) and a private address refers to a network address only visible privately within the network that assigned it. '859 patent, 1:16-32.

As described above, the purpose of the patent is to assign public and private network addresses in a GPRS network. The patent explains that, to conserve the IP addresses, "private addresses" can be used within an administrative domain:

> One of the limitations of IPv4 is that it has a limited address space. Consequently, ***in order to conserve addresses***, enterprises and other administrative domains (ADs) have ***resorted to using private addresses***. Private addresses are network addresses in which the IP address falls within the ranges of
>
> [10.0.0.0-10.255.255.255],
> [172.16.0.0-172.31.255.255], or
> [192.168.0.0-192.168.255.255].
>
> Private addresses that are assigned by an administrative entity within an administrative domain have relevance only within the administrative domain. Accordingly, ***such private addresses must not be visible outside the administrative domain***. An advantage of using private addresses is that different administrative domains may assign the same private IP address to hosts within their respective administrative domains without any concern of conflict.

Id. In sum, according to the patent, certain IP address ranges, which are defined by an Internet standard, can be used as "private addresses" that can be used within the particular network that they are assigned, but are not visible outside the network. Ex. 6 (RFC 1918) (defining the ranges of private IP addresses). This allows the network to conserve IP addresses because they do not need a public IP address for every single device in the network. The patent explains that, because private IP addresses are not visible outside of the network, networks that employ private IP addresses traditionally utilize a NAT to translate public addresses to specific private addresses.

'859 patent, 1:32-43, Fig. 1; *see* Ex. 7 (RFC 3022).

It is not clear what part of Cisco's proposed construction WSOU takes issue with.[4] As detailed above, Cisco's construction is fully consistent with the well-understood meaning of "private network address" and the intrinsic record. Cisco asked WSOU how the alleged "plain and ordinary meaning" was different than Cisco's construction during the parties' meet and confer, but WSOU could not articulate any substantive response.

Because Cisco's proposed construction is in line with the ordinary meaning of the term, and the specification's description of the term, it should be adopted.

III. U.S. Patent No. 8,191,106

The '106 patent relates generally to a network that allows users to connect using different access technologies (such as cellular, Wi-Fi, wired connection, etc.). The described network is able to detect when a user changes their access technology (*e.g.*, switches from cellular to Wi-Fi), and then applies a security policy specific to the new access technology.

According to the patent, existing security policies were specific to particular users. '106 patent, 1:36-39. Such policies, as the patent explains, were not equipped to handle the convergence between fixed networks (like Ethernet) and mobile networks (like cellular). *Id.*, 3:1-6. This is because a device connected via a fixed network may have different security requirements than a device connected via a mobile network. *Id.*, 2:7-29. This alleged problem would not arise where networks only had a single access type (*e.g.*, only fixed networks) because the user would always connect to that network with the same access type.

[4] WSOU initially disclosed "private network address" as a term needed for construction, but only proposed "plain and ordinary meaning" as its proposed construction. Ex. 8 (September 1, 2021 WSOU Proposed Terms For Construction).

To remedy this perceived deficiency specific to converged networks, the patent describes an "inter-technology change-off monitoring entity (ICME)" that detects when a device changes the access type through which it is connected to the converged network. When a change is detected, the ICME can choose a new security policy to apply based on the access type. This is illustrated in Figure 4, annotated below:

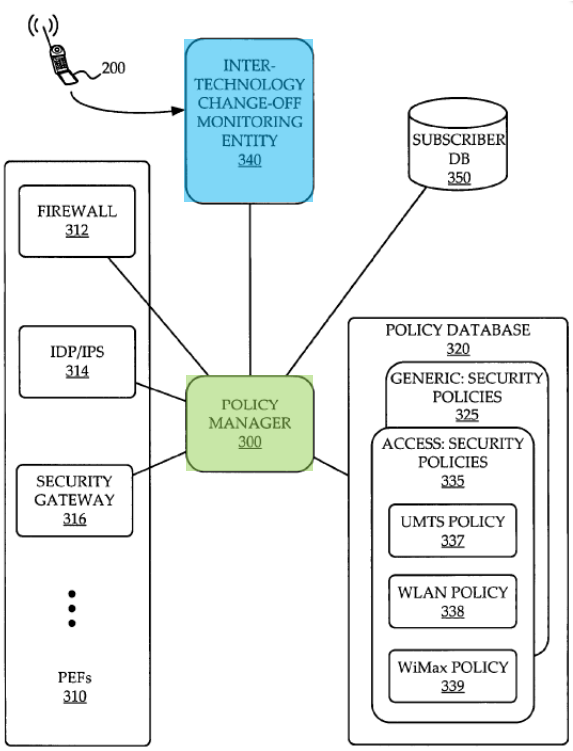

FIG. 4

As shown above, the converged network includes an ICME **340** that communicates with a policy manager **300**. When the ICME detects a change in access technology, it contacts the policy manager. The policy manager can then retrieve the appropriate security policy from a database **320** based on the access technology that the device is connected with. For example, the figure depicts different policies for different access technologies: UMTS **337**, WLAN **338**, and WiMax **339**.

A. "inter-technology change-off monitoring entity (ICME)" / "ICME" (Claims 1, 5-7, 10)

Cisco's Proposal	WSOU's Proposal
Entity that monitors the type of technology being used to access the converged network	Plain and ordinary meaning Alternatively, "hardware and/or software which monitors one or more access types"

Cisco's proposed construction is fully consistent with the language of the claim: "***[I]nter-technology*** change-off monitoring entity." WSOU's proposed construction, on the other hand, is a plain attempt to read the word "***inter-technology***" out of the claim. In the same way an "***inter***national" flight must be between two different countries, an "***inter***-technology change-off monitoring entity" must monitor a change-off between at least ***two*** different technologies. This is consistent with the well-understood meaning of the "inter-" prefix, meaning between or among. WSOU's suggestion that there only needs to be "one or more access types" is therefore contrary to the plain language of the claims. An entity that monitors only a single type of access is not "***inter***-technology."[5] By analogy, a flight within the U.S. is not "***inter***national"; it is domestic.

The claims and the specification confirm the plain meaning of "***inter-technology***" proposed by Cisco. For example, claim 1 recites that the ICME must "detect[] an inter-technology change-off of a multimodal device from a ***first access technology*** of the converged network to a ***second access technology*** of the converged network." This confirms that the "inter-technology change-off monitoring entity" must monitor a change off between two different access technologies as suggested by the plain meaning. The specification similarly recites: "Once the multimodal mobile

[5] In its infringement contentions, WSOU accuses Cisco products that only allow monitor access via a single access technology—Wi-Fi. *See* Ex. 1 (WSOU's Preliminary Infringement Contentions), Ex. C, 5-6; *Wilson Sporting Goods*, 442 F.3d at 1327.

device 200 ***starts to change the access technology*** it is using to access the converged fixed/mobile network, the ICME 340 monitors that ***the change in access technology*** is taking place." '106 patent, 7:61-64; *see id.*, 7:40 ("The ICME 340 monitors the type of access being used."). In other words, the totality of the intrinsic record supports Cisco's plain meaning construction.

WSOU's proposal, on the other hand, is inconsistent with the plain meaning of the term and the intrinsic record. There is no support for the notion that an "***inter-technology*** change-off monitoring entity" can be "hardware and/or software which monitors one or more access types." Indeed, this proposal would contradict the claims themselves which recite two different access technologies. *See* '106 patent, cl. 1.

B. "converged network" (Claims 1, 10)

Cisco's Proposal	WSOU's Proposal
Network with a common core that supports multiple access technologies including both fixed and mobile access technologies	Plain and ordinary meaning

Cisco's proposed construction of "converged network" comes directly from the intrinsic record, and requires a network that permits both fixed and mobile access to a single, common network core. The claims themselves require a first and second access technology "***of the converged network***." '106 patent, cl. 1. This means that the converged network must support ***at least two*** (*i.e.*, multiple) access technologies.

The specification expands on this, distinguishing converged networks from separate fixed and mobile networks:

> With the advent of IMS and the effort towards ***convergence between fixed and mobile networks***, the networks of the future will be drastically different. Independent "Mobile Core" and "Fixed Core" networks will be replaced with what is referred to as ***a converged network which has a common core connecting to different access technologies***.

Id., 2:7-13. In other words, as detailed by the patent, a "converged network" replaces separate mobile and fixed cores with a common core that allows access via multiple mobile and fixed access technologies.

The rest of the specification confirms this distinction between converged networks that need to determine through which access technology a device is connected, on the one hand, and separate mobile and fixed networks, on the other hand. For example, the Abstract states that "[t]he policy manager conveys to various policy enforcement points throughout the ***converged fixed/mobile network*** the applicable security policies which ***take into account*** the user's identity and ***the access technology being used***." The stated problem that the patent seeks to solve, moreover, is to "manage security in such a way that can accommodate multiple access technologies" in a "[c]onverged fixed/mobile network[]." *Id.*, 4:51-53. The summary of the invention and the detailed description likewise disclose that the purpose of the patent is for detecting change in access technology type on a converged network. *Id.*, 4:57-5:6, 6:56-8:17. In short, a converged network, as implied by the use of "converged" in the name, must have a common core network that supports at least two different access technologies including mobile and fixed networks.

Indeed, the stated purpose of the patent—to detect which access technology a device uses to connect to these converged networks (*e.g.*, fixed or mobile) so that the network can employ a different security policy based on the access technology (*id.*, 4:51-53, 4:57-5:6)—would make no sense in a network that has only a single access technology. There would be no point to having security policies based on access type if there were only a single access type—*e.g.*, only mobile or only fixed connections—confirming that a converged network must support multiple access technologies.

While WSOU provided no insight during meet and confer discussions as to the meaning of a converged network, WSOU's extrinsic evidence suggests that WSOU is seeking to encompass networks that handle different types of communication traffic (*i.e.*, voice, video, and data communications). Ex. 9 (Cisco Networking Academy). This extrinsic evidence is contrary to the use of the "converged network" in the patent described above and thus disfavored under *Phillips*. For example, a single-access-type network that handles voice, video, and data communications does not need different policies based on different access technologies. In direct contrast, the entire purpose of the patent is to allow different security policies for different access technologies in a converged network. Cisco therefore respectfully requests that the Court clarify the meaning of this term by adopting Cisco's proposal, which is consistent with the totality of the intrinsic record.

IV. U.S. Patent No. 8,989,216

The '216 patent relates to a Diameter command dictionary. '216 patent, 1:53-60. Diameter is a well-known computer networking protocol used for authentication, authorization, and accounting. *See* Ex. 10 (RFC 3588), 9. The Diameter protocol consists of commands and attribute value pairs ("AVPs"). Diameter commands convey messages between network nodes and deliver all data in the form of AVPs. *Id.* Each command may contain mandatory AVPs, which must be present in the command, and optional AVPs, which need not be present. *Id.* A Diameter dictionary—much like a regular dictionary—sets forth the definitions of commands and AVPs according to the Diameter protocol. '216 patent, 1:35-41. Applications use such a dictionary to translate and execute received commands and AVPs. *Id.*, 3:40-58.

One application for the Diameter protocol is for communication between nodes in a 3rd Generation Partnership Project ("3GPP") network. *Id.*, 1:19-20, 1:35-36. However, according to

the patent, 3GPP may on occasion change the Diameter command format when it releases new versions of a standard, potentially leading to incompatibility between different versions. *Id.*, 1:35-39.

To solve this alleged problem, the patent purports to describe the use of a single Diameter command dictionary that uses different definitions for commands and AVPs, depending on the particular context in which they are used. *Id.*, 1:53-60, 2:59-62, 3:9-12. For example, Figure 2 (annotated below) depicts a Diameter command dictionary with "context-specific" commands and AVPs:

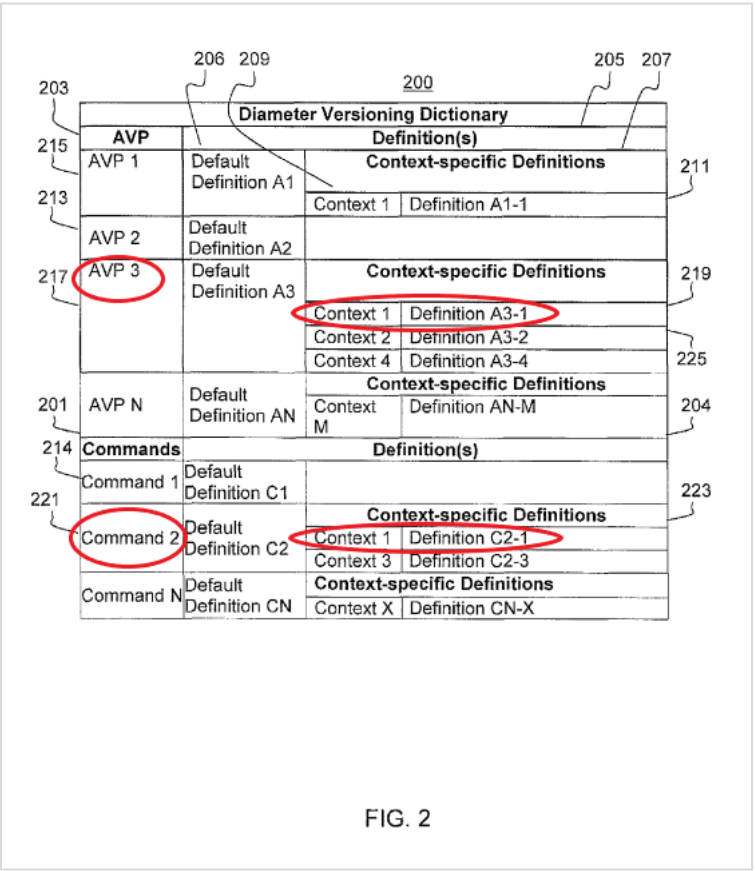

FIG. 2

As shown in Figure 2, each command and AVP has a "default" definition, along with one or more "context-specific" definitions that apply depending on the particular context. *Id.*, 2:63-3:31. For example, there may be different context-specific definitions provided for different versions of a

3GPP standard. *Id.*, 1:35-41. According to the patent, this use of context-specific commands and AVPs within a single dictionary allows the dictionary to address potential incompatibility between network nodes running on different versions of a standards release. *Id.*, 1:43-45.

The patent's purported solution is similar to a regular dictionary that may have different definitions of a word depending on the context. For example, the word "crane" could mean a bird, a machine, or an action depending on the context in which it is used. The '216 patent purports to merely apply that concept to Diameter dictionaries.

A. "context" (Claims 1, 2, 4, 5, 7, 9, 11, 12, 13, 14)

Cisco's Proposal	**WSOU's Proposal**
a specific condition to be met for the corresponding context-specific definition to apply	Plain and ordinary meaning

Cisco's proposed construction comes directly from the specification, where "context" is *explicitly defined*.

> Each context-specific definition (e.g., "Definition A1-1" 211) is indexed by a context (e.g., "Context 1" 29). ***A context identifies a specific condition to be met for the corresponding context-specific definition to apply***.

Id., 3:11-14.

Cisco's proposed construction of "context" is also consistent with the plain and ordinary meaning and is *verbatim* the specification's definition of the term. In a regular English dictionary, multiple definitions are often provided for a single word, depending on the context, *i.e.*, the specific condition that must be met for a specific definition to apply. For example, the default definition of the word "dough" refers to a mixture of solid and liquid ingredients for baking. In certain contexts, however, dough can be used to refer to money: "After I get paid on Friday, I'll have enough dough to go on vacation." The particular context in which the word is used dictates which definition applies to the word.

Cisco's proposed definition comes verbatim from this definition. A "'specification acts as a dictionary when it expressly defines terms'" in this manner. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005). In those circumstances, "there is no need to search further for the meaning of the term," and "that definition shall apply." *See Advanced Fiber Techs. v. J & L Fiber Servs., Inc.*, 674 F.3d 1365, 1372 (Fed. Cir. 2012); *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1478 (Fed. Cir. 1998). This definition of the term is entirely consistent with the term's use in the claims. *See e.g.*, '216 patent, 5:9-23, 6:16-27.

The prosecution history further confirms Cisco's proposed construction. Applicant describes: "For example, as shown in FIG. 2 accompanying the specification, a context may identify a specific condition to be met for the corresponding context-specific definition to apply. The context may include, *inter alia*, different versions and releases of the 3GPP standards and/or custom or proprietary implementation of specific vendors." *See* Ex. 11 ('216 Patent Prosecution History), 8. This language is identical to the express definition in the specification and Cisco's proposed construction.

For its part, WSOU has not identified anything incorrect about Cisco's proposed construction (nor could it, since the construction is lifted directly from the specification's definition of the term). As such, Cisco's proposal should be adopted.

B. "said specific context" / "said context" (Claims 2, 5, 7, 9)

Cisco's Proposal	WSOU's Proposal
Indefinite	Plain and ordinary meaning

The term "said specific context" is incurably indefinite because it is unclear which of the multiple contexts in the claim the disputed phrase refers to.

Claims 1 and 2, for example, recite:

> 1. A tangible non-transitory storage device readable by a machine, embodying a Diameter protocol command dictionary . . .
>
> wherein said Diameter protocol command is defined by a first default definition unless a ***first context*** applies . . .
>
> a second definition for a Diameter protocol attribute value pair (AVP), wherein said Diameter protocol or AVP is defined by a second default definition unless a ***second context*** applies. . .
>
> 2. The tangible non-transitory storage device of claim 1, wherein ***said specific context*** comprises a specific version of a 3rd Generation Partnership Project (3GPP) standard.

In other words, the claims recite a "first context" (green) and another "second context" (blue). The term at issue, however, refers to using a "***said specific context***" (red). Since there are two different recited "contexts," it is unclear to which context the "said specific context" refers. It could refer to either the first context or the second context. This lack of clarity renders the term indefinite.

The Federal Circuit recently affirmed indefiniteness of a similar term in *Bushnell Hawthorne, LLC v. Cisco Systems, Inc.*, 813 F. App'x 522, 526 (Fed. Cir. May 14, 2020). There, the claim recited three sets of different IP addresses. Later in the claim, the patent used the term "said ***different*** IP address," which lacked an antecedent basis. The Federal Circuit explained that, "[w]ith three different IP addresses to choose from, a POSA faced with the 'said different IP Address' limitation is left to wonder which of the different IP addresses is 'said' different one." *See id*. The same is true here. There are two different "contexts" to which the term "***said specific context***" could refer, with no guidance in the claims or specification as to which is referenced. "A POSA, faced with the claims and the specification, could not, with reasonable certainty, discern the meaning of the claim term." *Id.*, 527. *See also Qcue, Inc v. Digonex Tech. Inc.*, 2013 WL

4784120, at *12-13 (W.D. Tex. Sept. 5, 2013) (finding claims indefinite when it was not clear which "processor" was referred to when there were multiple processors in the claim). Since the term "said specific context" has multiple plausible antecedent bases in the claim, it is indefinite.

This Court has very recently construed similar terms in other WSOU patents as indefinite. In *WSOU Investments, LLC v. Google*, the claim referring to "the terminal," was found to be indefinite when such term could have referred to either a "mobile communication terminal" or "another communication terminal." No. 6:20-cv-00581-ADA, Dkt. No. 46 at 3 (W.D. Tex. June 2, 2021); *see also* Ex. 12 (U.S. Patent No. 7,304,563), 6:37-53. Similarly, in *WSOU Investments, LLC v. Huawei Tech. Co.*, this Court found the term "the message" to be indefinite when it could have referred to "a message to the upstream device," or "a message reporting the depth of the queue." No. 6:20-CV-533-ADA, Dkt. No. 64 at 14 (W.D. Tex. June 1, 2021); *see also* Ex. 13 (U.S. Patent No. 7,872,973), 8:2-24. Here, the term "said specific context" is indefinite for the same reasons.

In meet and confer discussions, Cisco asked WSOU whether "said specific context" should be interpreted to refer to the first context or the second context. WSOU has taken the position that "said context" refers to the "first context." Ex. 14 (September 29, 2021 E-mail). However, there is nothing in the language of the claims nor in the specification to support this construction over the alternative where "said specific context" refers to the "second context." Nor did WSOU point to any intrinsic evidence to support its alleged construction. *See id*.

C. "said command or AVP is defined by a second default definition" (Claim 4)

Cisco's Proposal	WSOU's Proposal
Indefinite	Plain and ordinary meaning

The term "said command or AVP is defined by a second default definition" is incurably indefinite because it is completely inconsistent with the remainder of the claim.

Claim 4 recites:

> 4. A network node comprising a Diameter protocol command dictionary comprising: a first definition for a Diameter protocol command, wherein said ***Diameter protocol command*** is defined by a first default definition unless a first context applies in which case said command is defined by a context-specific definition . . .
>
> a second definition for a Diameter protocol attribute value pair (AVP), wherein ***said command or AVP*** is defined by a ***second default definition*** unless a second context applies in which case said AVP is defined by a second context-specific definition.

This claim language is internally irreconcilable. The first phrase above (green) specifies that the ***command*** is defined by a first default definition or a context-specific definition. But then the second phrase above (blue) inexplicably specifies that "***said command or AVP***" is defined by a second default definition or a second context-specific definition. This makes no sense for two reasons. First, a POSA would not have known with reasonable certainty whether the second default definition (red) applies to (1) the claimed command or (2) the claimed AVP. Second, if the second default definition applies to the command, the command would then have ***two*** default definitions. A POSA would not know how a command can have two default definitions; if no contexts apply, there would be no way to determine which "default" definition should apply. As a result, there is simply no way to make sense of the disputed language that is consistent with the claims.

WSOU urges the Court to adopt the plain and ordinary meaning, but as discussed above, there is no plain and ordinary meaning that is intelligible. And WSOU has offered no corrective alternative construction. Because the intrinsic record "fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of" these terms, they are indefinite. *Nautilus, Inc. v. Biosig Instruments, Inc*., 572 U.S. 898, 901 (2014).

It is, of course, possible that inclusion of "said command" was a drafting error, improperly included by the patentees, and that the second definition should only refer to a definition for said AVP. However, the claim *as written* is unclear and therefore cannot be corrected by the Court. *See Hoganas AB v. Dressler Indus. Inc.*, 9 F.3d 948, 951 (Fed. Cir. 1993); *see also T-Rex Prop. AB v. Regal Entm't Grp.*, 2019 WL 4935264, at *4 (E.D. Tex. Mar. 5, 2019) (finding claim indefinite because "when considered in the context of the surrounding claim language, the claim does not make sense as drafted"). Accordingly, this term is indefinite.

V. U.S. Patent No. 9,357,014

The '014 patent generally relates to creating and maintaining service connections between endpoints. '014 patent, Abstract. According to the patent, endpoints are "devices which may communicate at the application layer." *Id*., 3:23-24. The '014 patent proposes replacing traditional networking connections between endpoints with "service connections" between endpoints. *Id*., 2:23-26. To enable service connections, the '014 patent describes replacing the traditional TCP/IP Stack or OSI Stack with a "connected services stack." Figure 2, annotated below, compares the connected services stack (highlighted in yellow) with the TCP/IP Stack and OSI Stack:

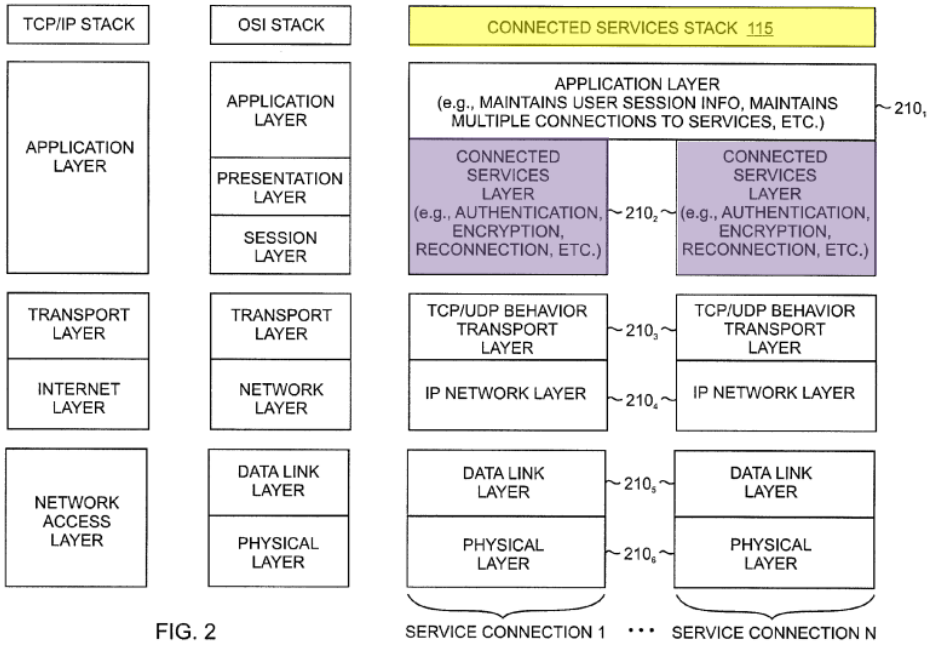

FIG. 2

As shown above, the connected services stack includes a "connected services layer [highlighted in purple] that is disposed below the application layer and above the transport layer." *Id.*, 1:33-36. The connected services layer supports establishment of a service connection between endpoints. *Id.*, 1:36-39. The patent further explains the process for establishing a service connection between endpoints using a message flow illustrated in Figure 3, annotated below.

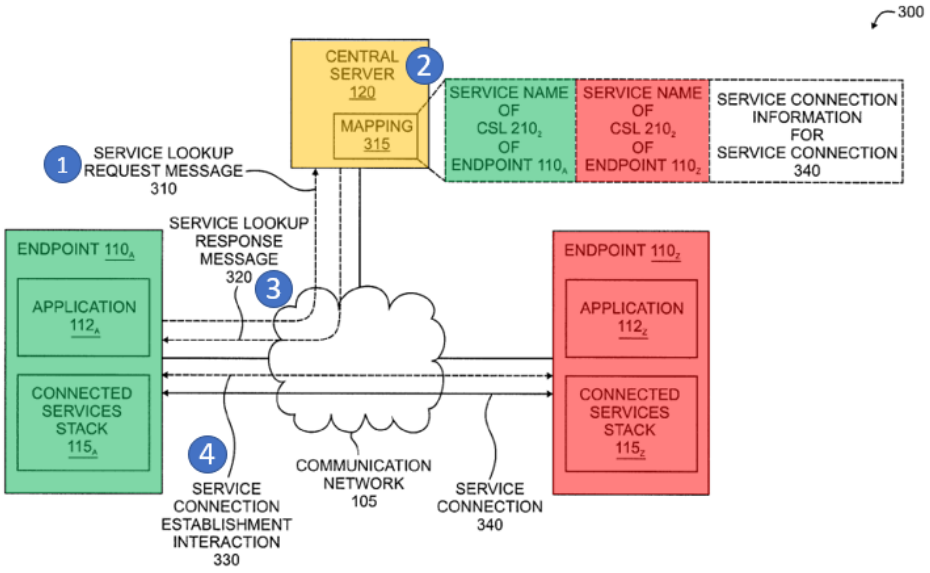

FIG. 3

Figure 3 above shows a **requesting endpoint 110_A**, a **remote endpoint 110_Z**, and a **central server 120**, and explains the sequence of steps to establish and use a service connection. *Id.*, 5:57-59.

At step (1), the connected services layer (CSL) of the connected services stack of requesting endpoint 110_A initiates a request for a service connection with remote endpoint 110_Z by sending a service lookup request message 310 to central server 120. *Id.*, 5:65-6:12. The service lookup request includes the service name of the CSL of the requesting endpoint 110_A ***and*** the service name of the CSL of the remote endpoint 110_Z. *Id.*, 6:19-26.

At step (2), the central server 120 stores a mapping 315 between the service names of the CSL of each endpoint and the service connection information for the service connection. *Id.*, 6:27-36.

At step (3), the central server 120 sends a service lookup response message 320 to the CSL of the requesting endpoint 110_Z, which includes service connection information for the service connection. *Id.*, 6:40-50. This information includes a service connection identifier for the service

connection, IP address of remote endpoint 110_Z, and the service name of the CSL of the endpoint 110_Z. *Id*.

At step (4), the CSL of the requesting endpoint 110_A communicates with the CSL of the remote endpoint 110_Z through the service connection establishment interaction 330 to establish a service connection 340 between the CSL of the requesting endpoint 110_A and the CSL of the remote endpoint 110_Z. *Id*., 6:51-7:43. Once established, the service connection 340 provides a connection between the two endpoints, via the connected services layer, that is above the transport layer and below the application layer. *Id*., 7:43-63.

A. "connected services layer" (Claims 1, 3-9, 12, 13, 15, 18, 19)

Cisco's Proposal	**WSOU's Proposal**
a layer that supports a service connection between two endpoints	Plain and ordinary meaning

Central to the '014 patent is the use of a "connected services layer"—a coined term that exists solely within the confines of the '014 patent. The intrinsic record uniformly describes the "connected services layer" as "a layer that supports a service connection between two endpoints." *3M Innovative Props. Co. v. Tredegar Corp.*, 725 F.3d 1315, 1321 (Fed. Cir. 2013) ("Idiosyncratic language, highly technical terms, or terms coined by the inventor are best understood by reference to the specification.").

The patent explains that the connected services layer is "configured to ***support*** establishment of a service connection." '014 patent, 1:35-38; *see also id*., 2:31-36, 4:26-29 ("support service-based networking"), 5:65-6:7 ("initiates a request for establishment of a service connection"), 6:51-7:37 (explaining how the connected services layer supports the service connection). The language of Cisco's proposed construction comes directly from those descriptions.

The connected services layer also allows for the endpoints to communicate through its support of the service connection between endpoints:

> The service connection establishment interaction **330** between [the connected services layers] results in establishment of the service connection therebetween (which is indicated as service connection **340** in FIG. 3). Here, again, it is noted that the service connection **340** is a connection between [the connected services layers] of the endpoints . . . .

The connected services layer also supports the service connection between endpoints by performing additional features such as authentication, encryption, reconnection or retransmission, and timeout handling. *Id*., 4:29-34, 7:46-56 (encryption), 8:36-47 (encryption), 9:18-20 (authentication), 9:23-29 (timeouts), 9:30-45 (packet retransmission).

The patent also describes the alleged benefits of a "connected services layer" as supporting a service connection. *See CVI/Beta Ventures, Inc. v. Tura LP*, 112 F.3d 1146, 1160 (Fed. Cir. 1997) (construction should be "consistent with and further[] the purpose of the invention"). According to the specification, with a connected services layer, applications and services (*i.e.*, at the application layer) need not have knowledge about their underlying service connection. '014 patent, 4:34-60. Instead, the connected services layer provides support for the service connection—it handles connectivity or failure of the service connection by "maintaining service connections," handling retransmission timeouts, and handling IP address changes. *Id*.; *see also id*., 9:46-60 (IP address changes), 9:61-10:39 (soft IP address change), 10:40-11:47 (hard IP address change). Thus, the '014 patent uniformly and consistently describes a "connected services layer" as "a layer that supports a service connection between two endpoints."

WSOU's position that the term should not be construed ignores that "connected services layer" is a coined term and has no plain and ordinary meaning outside of this patent. The reason is clear: WSOU wants to avoid construing the term so it can try to read it on products that have

no concept of a layer that sits between the application and transport layer. Tellingly, WSOU has not and cannot explain the "plain and ordinary meaning" of "connected services layer." And the jury should not be left to guess what a "connected services layer" is when the specification is clear about what it means.

The prosecution history also suggests that "connected services layer" does not have an understood meaning in the field. The applicants did not submit an information disclosure statement identifying any art in the field that use the term "connected services layer." During prosecution, the examiner cited four patents and patent publications—none of these documents use the term "connected services layer." *Id*., References Cited.

Finally, the parties' extrinsic evidence also does not show that "connected services layer" has an understood meaning in the field. For example, Cisco provided a textbook from July 2014 discussing networking communications. Ex. 15 (Guide to OSI and TCP/IP Models). This book does not discuss a "connected services layer." WSOU provided a copy of the AWS Lambda website. Ex. 16 (AWS Lambda). Notwithstanding that this website is from 2021, seven years *after* the filing date of the '014 patent, the website also does not use the term "connected services layer." Thus, there is no evidence that the "connected services layer" was known or readily understandable to a POSA—it is a coined term. *See Malvern Panalytical, Inc. v. TA Instruments-Waters LLC*, No. CV 19-2157-RGA, 2021 WL 965684, at *5 (D. Del. Mar. 15, 2021) (finding term was "coined" when Plaintiff did not show it had an "ordinary and customary meaning").

Because the meaning of "connected services layer" cannot be deciphered by its constituent words, it requires construction. *See Fintiv, Inc. v. Apple Inc.*, No. 18-CV-00372-ADA, Dkt. 86 (W.D. Tex. Nov. 27, 2019) (explaining when coined terms require construction). As a result, the Court should reject WSOU's plain and ordinary proposal and adopt Cisco's construction, which

succinctly and accurately captures the meaning of "connected services layer" in the '014 patent.

B. "service name of the connected services layer" (Claims 1, 18, 19)

Cisco's Proposal	WSOU's Proposal
service name of the requesting connected services layer	Plain and ordinary meaning

The parties' dispute centers on whether the "service name of the connected services layer" must be the service name of the connected services layer belonging to the *requesting* endpoint (Cisco's position) or whether it could be the service name of *any* connected services layer, including the service name of the connected services layer of the *remote* endpoint (WSOU's position).

The plain language mandates that the "service name of the requesting connected services layer" refers to the service name of the connected services layer belonging to the requesting endpoint. Claim 1 (annotated) recites:

> 1. An **apparatus**, comprising:
>
> a processor and a memory communicatively connected to the processor, the processor configured to run a connected services stack, the connected services stack comprising **a connected services layer** configured to operate below an application layer and above a transport layer, wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and **a *remote* connected services layer of a remote endpoint**, wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection, wherein the connected services layer is configured to:
>
> send, toward a server, a service connection request message comprising **the service name of the connected services layer** and **the service name of the remote connected services layer of the remote endpoint**; and
>
> receive, from the server, a service connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection.

In claim 1, the apparatus is the "requesting" endpoint because it is sending a message to the server. The claimed "apparatus" has a "connected services layer" (green) that is connected to a "remote connected services layer" (red). Each time the claim refers to "the connected services layer" it refers to the ***requesting*** connected services layer. Each time the claim refers to the "remote connected services layer" it refers to the connected services layer of the ***remote*** endpoint. Indeed, when the claim refers to the "service name of the connected services layer" it follows that immediately with a reference to the "service name of the remote connected services layer." That juxtaposition makes it unambiguously clear that "the service name of the connected services layer" is referring to the name of the requestor, not the name of the remote endpoint. Cisco's proposed construction merely makes it clear to the jury which endpoint is referred to.

Cisco's proposed construction is also consistent with the intrinsic record. The '014 patent describes how one endpoint ("requesting endpoint") initiates a service connection with a second endpoint ("remote endpoint") by sending a message lookup request message to a central server. *E.g.*, '014 patent, Fig. 3, 5:65-6:12. That lookup request contains "a service name of the CSL **210**$_2$ of CSS **115**$_A$ at endpoint **110**$_A$ ['requesting endpoint'], ***and*** a service name of the CSL **210**$_2$ of CSS **115**$_Z$ at endpoint **110**$_Z$ ['remote endpoint']."

Thus, the Court should reject WSOU's position (which essentially allows the claim to refer to the service name of *any* connected services layer) and instead construe "service name of the connected services layer" as service name of the ***requesting*** connected services layer.

Date: October 6, 2021

Respectfully Submitted,

/s/Brian Rosenthal with permission, by Michael E. Jones

Michael E. Jones
SBN: 10929400
POTTER MINTON
110 North College, Suite 500
Tyler, TX 75702
mikejones@potterminton.com
Telephone: (903) 597-8311
Facsimile: (903) 593-0846

Brian Rosenthal
Katherine Dominguez
Allen Kathir
Admitted *pro hac vice*
brosenthal@gibsondunn.com
kdominguez@gibsondunn.com
akathir@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166
Tel: (212) 351-4000

Ryan Iwahashi
Admitted *pro hac vice*
riwahashi@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1881 Page Mill Road
Palo Alto, CA 94304
Tel: (650) 849-5367

Kenneth G. Parker
kparker@gibsondunn.com
GIBSON, DUNN AND CRUTCHER LLP
3161 Michelson Drive
Irvine, CA 92612
Tel: (949) 451-4336

Attorneys for Defendant Cisco Systems, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that on October 6, 2021, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document through the Court's CM/ECF system under Local Rule CV-5(b)(1).

/s/ Brian Rosenthal
Brian Rosenthal